20STO: 9765960

TITLE: METHOD AND APPARATUS FOR PERFORMING MODULAR MULTIPLICATION
INVENTOR(S): MICHAEL D. RUEHLE
ATTY. DOCKET NO.: 042390.P11975

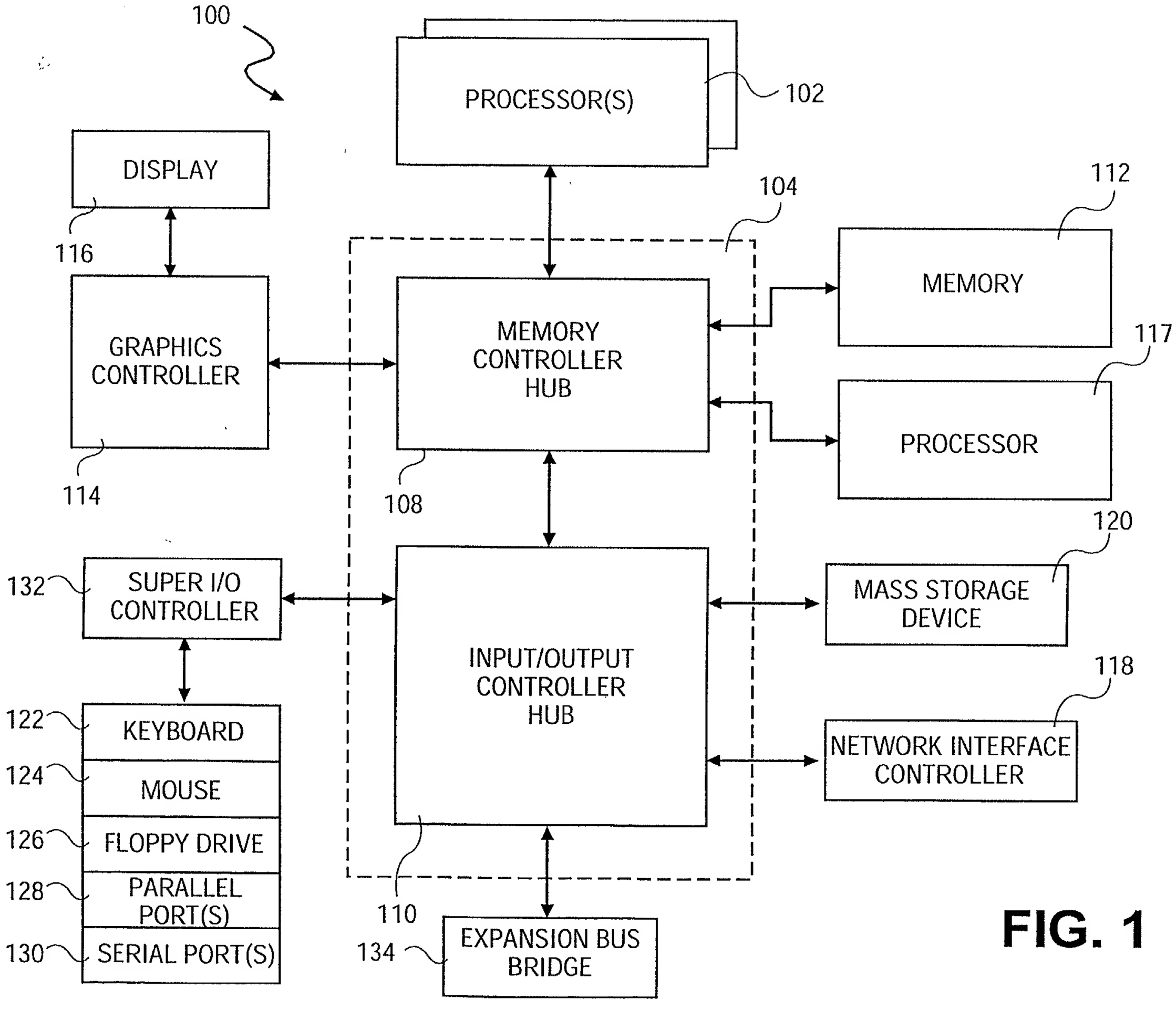

FIG. 1

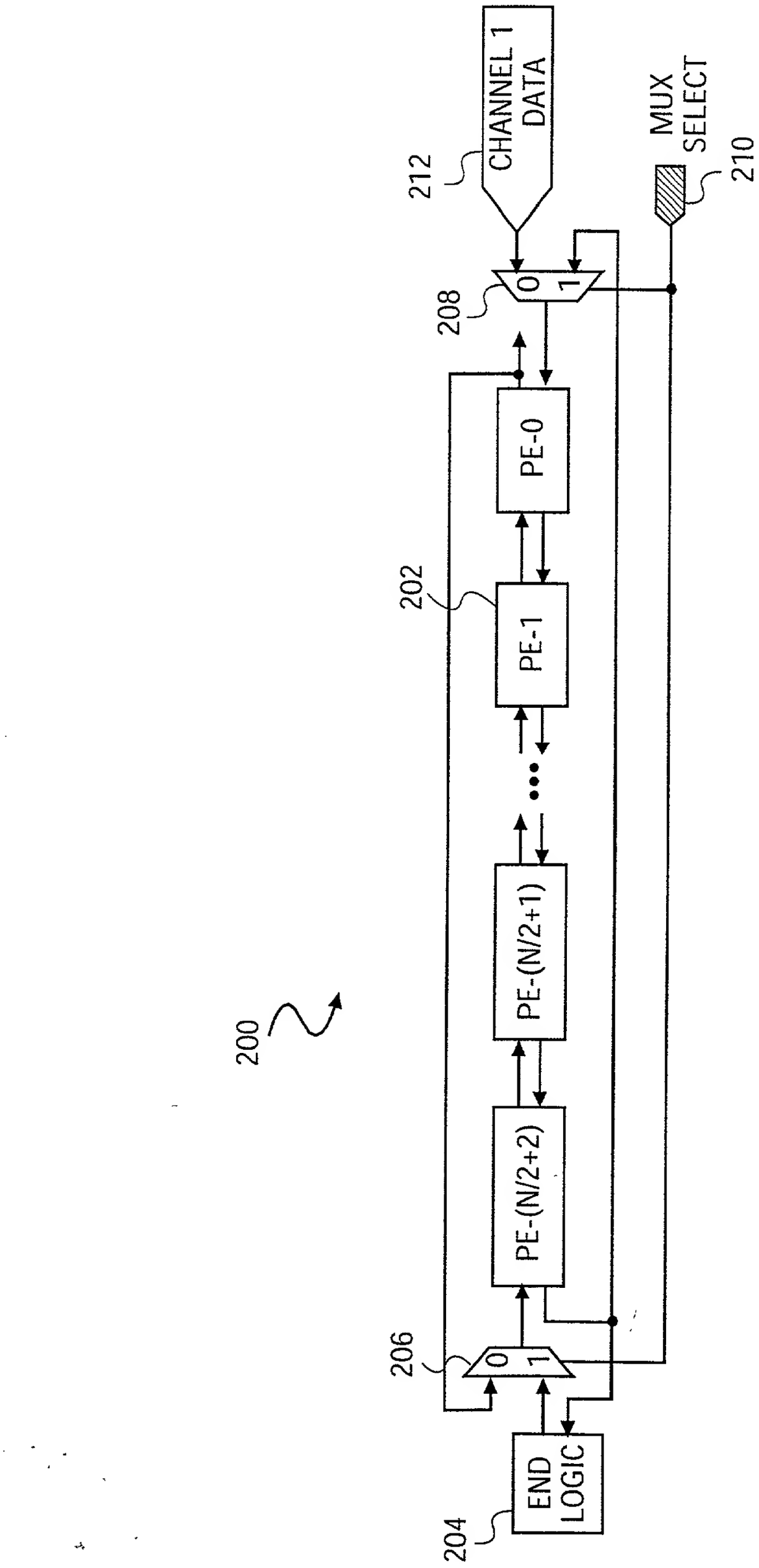
200
202
204
206
208
210
212
CHANNEL 1 DATA
MUX SELECT
PE-0
PE-1
PE-(N/2+1)
PE-(N/2+2)
END LOGIC
0
1

FIG. 2

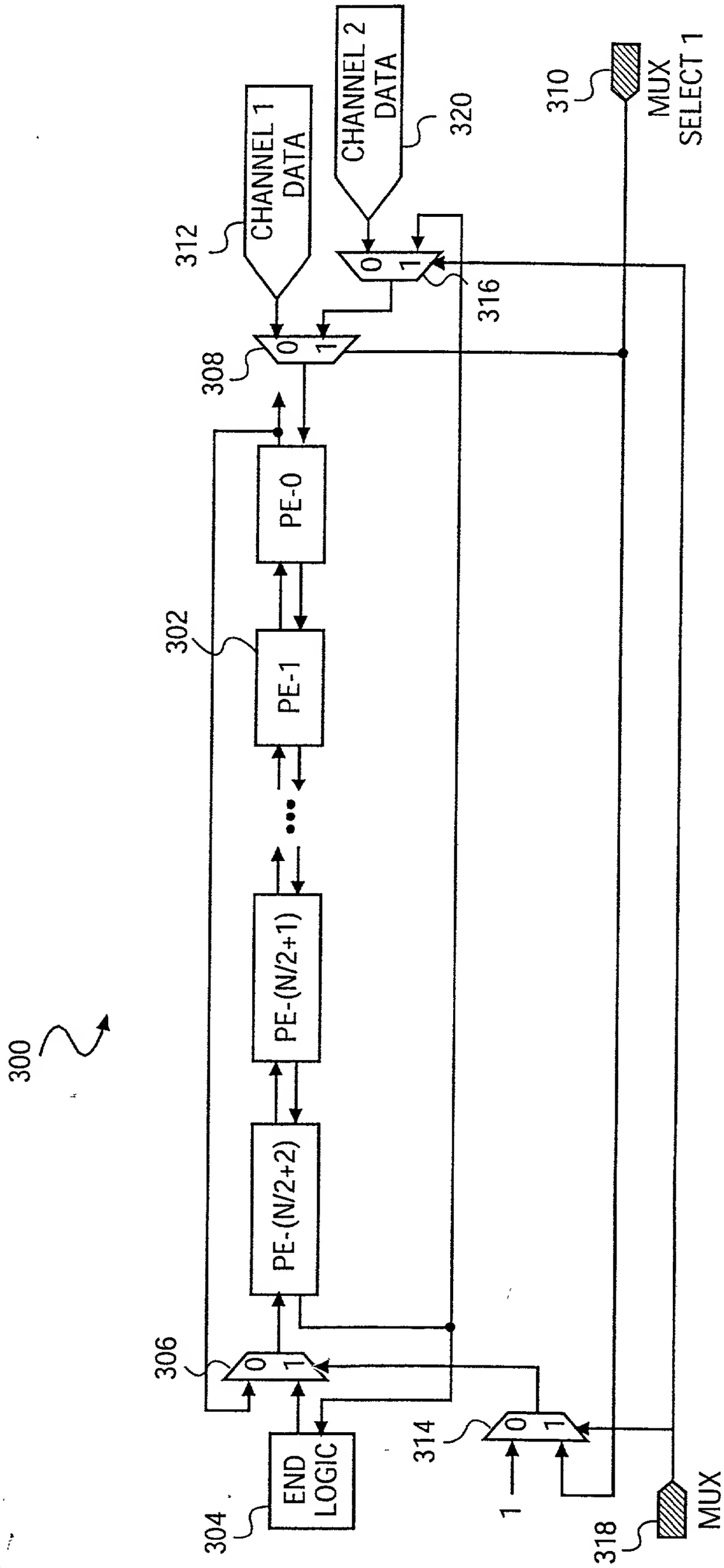
300
302
304
306
308
310
312
314
316
318
320
CHANNEL 1 DATA
CHANNEL 2 DATA
MUX SELECT 1
MUX SELECT 2
END LOGIC
PE-0
PE-1
PE-(N/2+1)
PE-(N/2+2)
0
1

FIG. 3

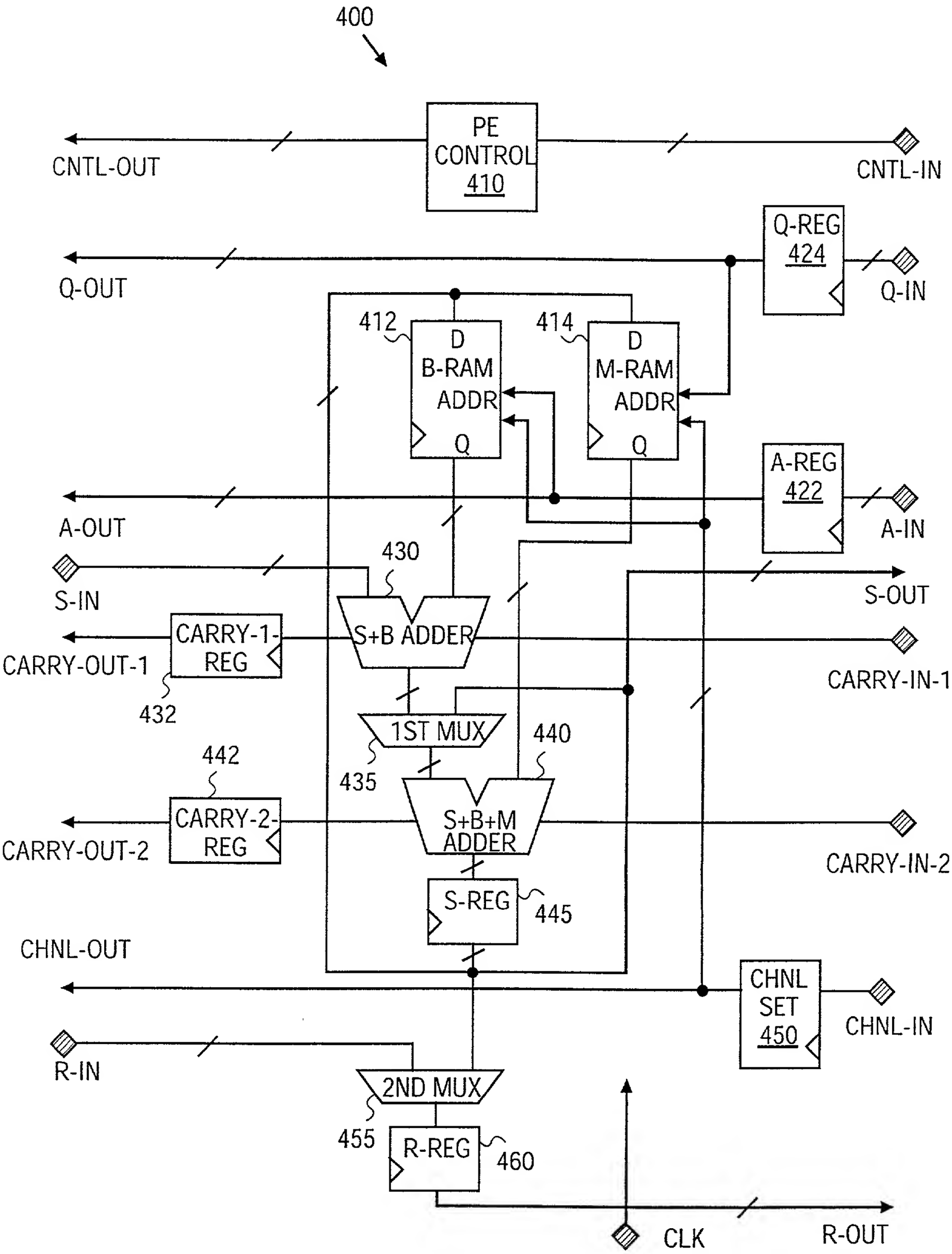
400
PE CONTROL 410
CNTL-OUT
CNTL-IN
Q-REG 424
Q-OUT
Q-IN
412
D B-RAM ADDR Q
414
D M-RAM ADDR Q
A-REG 422
A-OUT
A-IN
430
S-IN
S-OUT
CARRY-1-REG
S+B ADDER
CARRY-OUT-1
CARRY-IN-1
432
1ST MUX
435
440
442
CARRY-2-REG
S+B+M ADDER
CARRY-OUT-2
CARRY-IN-2
S-REG
445
CHNL-OUT
CHNL SET 450
CHNL-IN
R-IN
2ND MUX
455
R-REG
460
CLK
R-OUT

FIG. 4

TITLE: METHOD AND APPARATUS FOR PERFORMING MODULAR MULTIPLICATION
INVENTOR(S): MICHAEL D. RUEHLE
ATTY. DOCKET NO.: 042390.P11975

CYCLE	MUX SELECT	END LOGIC	PE-6	PE-5	PE-4	PE-3	PE-2	PE-1	PE-0	INPUT REGS
1	0								0	
2	1						2	1	0	
3	0					3	2	1	0	
4	1				4	3	2	1	0	
5	0			5	4	3	2	1	0	
6	1		6	5	4	3	2	1	0	
7	0		6	5	4	3	2	1	0	
8	1		6	5	4	3	2	1	0	
9	0		6	5	4	3	2	1	0	
10	1		6	5	4	10	2	1	0	
11	0		6	5	4	10	2	1	0	
12	1		6	5	4	10	2	1	0	
13	0		6	5	4	10	2	1	0	
14	1		6	5	4	10	2	1	0	
15	0		13	12	11	10	9	8	7	
16	1		13	12	11	10	9	8	7	
17	0		13	12	11	10	9	8	7	
18	1		13	12	11	10	9	8	7	
19	0		13	12	11	10	9	8	7	
20	1		13	12	11	10	9	8	7	

FIG. 5

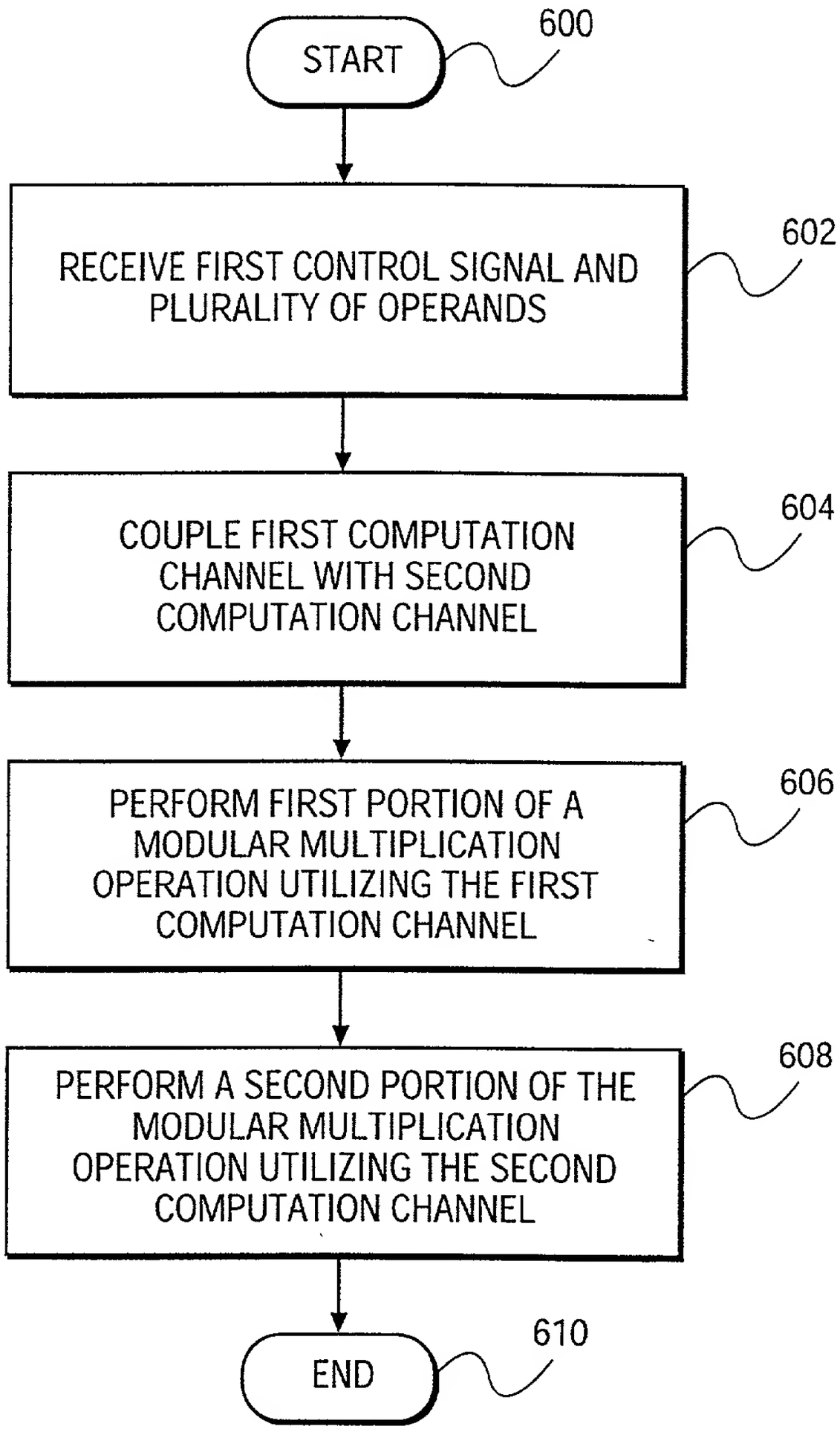
START
600
RECEIVE FIRST CONTROL SIGNAL AND PLURALITY OF OPERANDS
602
COUPLE FIRST COMPUTATION CHANNEL WITH SECOND COMPUTATION CHANNEL
604
PERFORM FIRST PORTION OF A MODULAR MULTIPLICATION OPERATION UTILIZING THE FIRST COMPUTATION CHANNEL
606
PERFORM A SECOND PORTION OF THE MODULAR MULTIPLICATION OPERATION UTILIZING THE SECOND COMPUTATION CHANNEL
608
END
610

FIG. 6